KILE PARK GOEKJIAN REED & MCMANUS PLLC

ATTORNEYS AT LAW

1200 NEW HAMPSHIRE AVENUE, N. W., SUITE 570
WASHINGTON, D.C. 20036 USA
TELEPHONE (202) 659-8000
FACSIMILE (202) 659-8822

FACSIMILE TRANSMITTAL SHEET

Application No.: 10/582,127	**Confirmation No.: 2190**
Applicant(s): Dong-Hyuk Lee.	**Examiner: Khoshnoodi, Nadia (Art unit 2437) [Fax No. 571-273-3825]**
Title: FLEXIBLE NETWORK SECURITY SYSTEM AND METHOD FOR PERMITTING TRUSTED PROCESS	
Atty Docket No.: CMP-0008-SE	
Date: 11/14/2011	**Total Pages (including cover): 6**
Re: Proposed amendments to the claims for interview with Examiner.	

☐ URGENT ☒ FOR REVIEW ☐ PLEASE COMMENT ☐ PLEASE REPLY ☐ PLEASE RECYCLE

Dear Examiner Khoshnoodi,

Attached please find proposed amendments to the claims of the present application. I would like to request a telephone interview to discuss about the amended claims. I will call you on Monday (11/14/2011) to see your availability.

Thank you.

Jae Y. Park

Attorney for Applicant
Reg. No. 62629
Tel. No.: 202-263-0809

Application No. 10/582,127
Atty Docket CMP-0008-SE
Examiner: Nadia Khoshnoodi

Proposed Amendments to Claims for Examiner Interview

1. (Currently amended) A network security system for permitting a trusted process using a firewall, the firewall protecting a corresponding network connection of a computer to a network by setting restrictions on information communicated between networks, comprising:

a port monitoring unit [[for]] extracting information about a server port being used by a network communication program;

an internal permitted program storage [[for]] storing a list of programs permitted ~~to have server ports registered~~ by the firewall, wherein the internal permitted program storage adds a program to the list by extracting information about the program for which communication is to be permitted by the firewall ~~and registering the extracted information in the list~~; and

a firewall flexible device [[for]] determining whether the network communication program is registered in the list of programs stored in the internal permitted program storage; [[and]]

~~an internal permitted port storage registering~~ wherein the firewall flexible device automatically storing the extracted information about the server port in an internal permitted port storage if ~~the firewall flexible device determines that~~ the network communication program is registered in the list of programs stored in the internal permitted program storage; and

wherein the firewall flexible device further determines whether a destination port of a packet of inbound traffic ~~has been registered in the internal permitted port storage~~matches with the server port and blocks the packet of inbound traffic if the destination port ~~has not been registered~~does not match with the server port.

2. (Currently amended) The network security system as set forth in claim 1, wherein the information about the program, ~~which is extracted and registered in the internal permitted program storage,~~ includes information about at least one of a program name, an entire path of the program, and a program hash value.

3. (Currently amended) The network security system as set forth in claim 1, wherein the information about the server port~~, which is registered in the internal permitted port storage,~~ includes information about at least one of an entire path of the program, a protocol, and a port.

4. (Currently amended) A network security method of permitting a trusted process using a firewall, the firewall protecting a corresponding network connection of a computer to a network by setting restrictions on information communicated between networks, comprising:

storing in an internal permitted program storage a list of programs permitted ~~to have server ports registered~~ by the firewall;

extracting information about a server port being used by a network communication program;

Formatted
Formatted: Line spacing: Multiple 1.15 li
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted

determining whether the network communication program is registered in the list of programs stored in the internal permitted program storage;

~~registering~~automatically storing the extracted information about the ~~extracted~~ server port in an internal permitted port storage if the network communication program is ~~determined to be~~ registered in the list of programs stored in the internal permitted program storage;

determining whether a destination port of a packet of inbound traffic ~~has been registered in the internal permitted port storage~~matches with the server port; and

blocking the packet of inbound traffic if the destination port ~~has not been registered~~does not match with the server port.

5 - 7. (Canceled)

8. (Previously presented) The network security method as set forth in claim 4, wherein the information about the program includes information about at least one of a program name, an entire path of the program, and a program hash value.

9. (Currently amended) The network security method as set forth in claim 4, wherein the information about~~of~~ the server port includes information about at least one of an entire path of the program, a protocol, and a port.

10. (Currently amended) A computer recordable device for performing a network security method using a firewall, the device storing a program for executing the method, the method comprising:

storing in an internal permitted program storage a list of programs permitted ~~to have server ports registered~~ by the firewall;

extracting information about a server port being used by a network communication program;

determining whether the network communication program is registered in the list of programs stored in the internal permitted program storage;

~~registering~~automatically storing the extracted information about the ~~extracted~~ server port in an internal permitted port storage if the network communication program is ~~determined to be~~ registered in the list of programs stored in the internal permitted program storage;

determining whether a destination port of a packet of inbound traffic ~~has been registered in the internal permitted port storage~~matches with the server port; and

blocking the packet of inbound traffic if the destination port ~~has not been registered~~does not match with the server port.

Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted

11. (Currently amended) The network security system as set forth in claim 1, wherein the firewall flexible device allows the packet of inbound traffic to bypass the firewall if the destination port ~~has been registered~~matches with the server port.

12. (Currently amended) The network security method as set forth in claim 4, further comprising:

allowing the packet of inbound traffic to bypass the firewall if the destination port ~~has been registered~~matches with the server port.

13. (Currently amended) The network security system as set forth in claim 1, wherein the ~~internal permitted port storage registers~~ firewall flexible device stores the extracted information about the server port if the server port is determined to be opened.

14. (Previously presented) The network security system as set forth in claim 1, wherein the extracted information about the server port is deleted from the internal permitted port storage if the server port is determined to be closed.

15. (Currently amended) The network security method as set forth in claim 4, further including:

~~registering~~storing the extracted information about the sever port in the internal permitted port storage if the server port is determined to be opened.

16. (Previously presented) The network security method as set forth in claim 4, further including:

deleting the extracted information about the sever port from the internal permitted port storage if the server port is determined to be closed.

17. (Currently amended) The computer recordable device as set forth in claim 10, wherein the method further including:

~~registering~~storing the extracted information about the sever port in the internal permitted port storage if the server port is determined to be opened.

18. (Previously presented) The computer recordable device as set forth in claim 10, wherein the method further including:

deleting the extracted information about the sever port from the internal permitted port storage if the server port is determined to be closed.

Formatted
Formatted
Formatted
Formatted
Formatted: Font color: Auto
Formatted
Formatted
Formatted: Font color: Auto

19. (New) A network security system for permitting a trusted process using a firewall, the firewall protecting a corresponding network connection of a computer to a network by setting restrictions on information communicated between networks, comprising:

a port monitoring unit extracting information about a server port being used by a network communication program;

an internal permitted program storage storing a list of programs permitted by the firewall, wherein the internal permitted program storage adds a program to the list by extracting information about the program for which communication is to be permitted by the firewall; and

a firewall flexible device determining whether the server port is opened or closed and whether the network communication program is registered in the list of programs stored in the internal permitted program storage;

wherein the firewall flexible device automatically storing the extracted information about the server port in an internal permitted port storage if the server port is opened and the network communication program is registered in the list of programs stored in the internal permitted program storage;

wherein the firewall flexible device determines whether a destination port of a packet of inbound traffic matches with the server port and blocks the packet of inbound traffic if the destination port does not match with the server port.

20. (New) The network security system as set forth in claim 19,

wherein the firewall flexible device deletes the extracted information about the server port from the internal permitted port storage if the server port is determined to be closed.

21. (New) The network security system as set forth in claim 19,

wherein the information about the program includes information about at least one of a program name, an entire path of the program, and a program hash value.

22. (New) The network security system as set forth in claim 19, wherein the information about the server port includes information about at least one of an entire path of the program, a protocol, and a port.

23. (New) A network security method of permitting a trusted process using a firewall, the firewall protecting a corresponding network connection of a computer to a network by setting restrictions on information communicated between networks, comprising:

storing in an internal permitted program storage a list of programs permitted by the firewall;

extracting information about a server port being used by a network communication program;

Formatted
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted: (Asian) Korean
Formatted
Formatted
Formatted
Formatted: Font: Not Bold
Formatted
Formatted
Formatted: Line spacing: Multiple 1.15 li
Formatted
Formatted
Formatted
Formatted: Line spacing: Multiple 1.15 li
Formatted
Formatted
Formatted: Line spacing: Multiple 1.15 li

determining whether the network communication program is registered in the list of programs stored in the internal permitted program storage and whether the server port is opened or closed;

automatically storing the extracted information about the server port in an internal permitted port storage if the network communication program is registered in the list of programs stored in the internal permitted program storage and the server port is opened;

determining whether a destination port of a packet of inbound traffic matches with the server port; and

blocking the packet of inbound traffic if the destination port does not match with the server port.

24. (New) The network security method as set forth in claim 23, wherein the method further comprises deleting the information about the server port used by the network communication program if the server port is determined to be closed.

25. (New) The network security method as set forth in claim 23, wherein the information about the program includes information about at least one of a program name, an entire path of the program, and a program hash value.

26. (New) The network security method as set forth in claim 23, wherein the information of the server port includes information about at least one of an entire path of the program, a protocol, and a port.

27. (New) The firewall as set forth in claim 16,

wherein the firewall flexible device allows the packet of inbound traffic to bypass the firewall if the destination port matches with the server port.

28. (New) The method as set forth in claim 20, further comprising:

allowing the packet of inbound traffic to bypass the firewall if the destination port matches with the server port.

Formatted
Formatted
Formatted: Line spacing: Multiple 1.15 li
Formatted
Formatted
Formatted
Formatted
Formatted: Line spacing: Multiple 1.15 li
Formatted
Formatted
Formatted
Formatted
Formatted
Formatted